Szendrei Ferenc

A KIBERTÉRBEN FOLYTATOTT HUMÁN INFORMÁCIÓSZERZÉS LEHETŐSÉGEI

Nagy örömmel fogadtam a megtisztelő felkérést, hogy „ezeréves" kollégám, Balla Zoltán tanár úr – aki ebből az ezerből akár tízet is simán letagadhat – születésnapja alkalmából megjelenő ünnepi kötetbe írjak egy cikket, ezzel is tisztelegve a rendőrképzésben betöltött helye, szakmai és oktatói kvalitásai és emberi nagysága előtt. Gratulálok ehhez az évfordulóhoz, és bízom benne, hogy még sokáig velünk lesz és folytatja oktatói-kutatói pályafutását.

A 21. század robbanásszerű technológiai fejlődése, a digitális társadalom kialakulása és egyre növekvő szerepe újabb és újabb kihívások elé állítja a bűnüldöző szerveket. A kiberfenyegetések egyre célzottabbá, professzionálisabbá és komplexebbé válnak, tömegesen jelennek meg kifinomult zsarolóvírus-támadások, a számítógépes rendszerek sebezhetőségeinek kihasználása, az identitáslopások, illetve más, esetenként újabb és újabb kiberbűncselekmények. A fenyegetettség fokozódása megköveteli az állami – köztük a bűnüldöző – szervek részéről a proaktív, hírszerzési információkra alapozott kiberbiztonsági stratégiát és fellépést. A kibertér stratégiai fontosságúvá vált az információszerzés terén. A humán információszerzés a kibertérben új dimenziókat nyithat meg olyan módszerekkel, amelyek ötvözik a tradicionális humánforrás-alapú adatgyűjtést a digitális eszközök nyújtotta lehetőségekkel. A cikk a terjedelmi korlátok miatt inkább csak gondolatébresztő szándékkal készült, a szerző szándéka szerint további publikációk alapja lehet.

JOGI HÁTTÉR

(1) 2025-ben Magyarország új kiberbiztonsági stratégiát fogadott el, amelynek rendeltetése az elektronikus információs rendszerek védelmének erősítése, a kritikus

DOI: https://doi.org/10.36250/01332_19 · ORCID: https://orcid.org/0000-0002-7890-913X

infrastruktúrák biztonságának garantálása, valamint az állami és magánszféra együttműködésének fokozása. Biztosítja az adatok bizalmasságát, sértetlenségét és rendelkezésre állását, hozzájárulva az ország és az EU versenyképességéhez és ellenálló képességéhez. Célja a digitális jólét és a nemzeti kiberbiztonsági ellenálló képesség erősítése és fenntartása.[1] A Stratégiában megfogalmazott célok elérése érdekében a Kormány számít a Rendőrség információs rendszerekkel összefüggő bűncselekmények megelőzésére, felderítésére hivatott szervezeteire, mint például a kiberbűncselekmények felderítésére és nyomozására feljogosított szervezetre.

(2) A Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény szerint társadalmi elvárás az állam és polgárai számára elengedhetetlen elektronikus információs rendszerekben kezelt adatok és információk bizalmassága, sértetlensége és rendelkezésre állása zárt, teljes körű, folytonos és a kockázatokkal arányos védelmének biztosítása, ezáltal a kibertér védelme, amely hozzájárul Magyarország biztonságához, ellenálló képességének és versenyképességének növeléséhez. A digitális fejlődés a digitális fenyegetettségek körének bővüléséhez is vezetett, ami akadályozhatja a gazdasági tevékenységek folytatását, pénzügyi veszteséget okozhat, és aláásható a felhasználók bizalmát, ezzel jelentős károkat okozva a gazdasági és társadalmi életben.

(3) A Büntető Törvénykönyv[2] (a továbbiakban: Btk.) határozza meg azokat a bűncselekményeket, amelyeket a kiberbűncselekmények körébe sorolhatunk. Ezen túlmenően számos hagyományos bűncselekmény valósulhat meg a kibertérben.

a) Informatikai rendszer elleni támadások:
- jogtalan hozzáférés *(hacking)*, illegális belépés egy rendszerbe;[3]
- rendszerbe való jogtalan beavatkozás (például DDoS-támadás, megszakítás);[4]
- adatok jogtalan törlése, módosítása vagy hozzáférhetetlenné tétele.[5]

b) Tiltott adatszerzés:
- információs rendszerben kezelt adatok jogosulatlan titkos megismerése (például lehallgatás, adatlopás);[6]

c) Számítástechnikai eszközök felhasználása:
- jogellenes eszközök előállítása vagy terjesztése (például jelszavak, behatoláshoz használható programok).[7]

1 1089/2025. (III. 31.) Korm. határozat Magyarország Kiberbiztonsági Stratégiájáról.
2 2012. évi C. törvény a Büntető Törvénykönyvről.
3 Btk. 423. §.
4 Btk. 423. §.
5 Btk. 423. §.
6 Btk. 422. §.
7 Btk. 424. §.

d) Online tartalommal kapcsolatos bűncselekmények:
- gyermekpornográfia előállítása, terjesztése, a gyerekek online zaklatása;[8]
- szerzői jogok megsértése, technológiai védelem kijátszása;[9]
- plágium, hamisítás.[10]

e) Információs rendszerek segítségével elkövetett csalások és hamisítások:
- számítógépes csalás vagy hamisítás; kártyás és online fizetési csalás;[11]
- számítógéppel elkövetett személyazonosság-lopás (például *identity fraud*);[12]
- spam küldése (nem büntetendő).

f) Egyéb – gyakran a kibertérben is megvalósuló – bűncselekmények:
- kábítószerekkel összefüggő bűncselekmények;[13]
- tiltott szerek forgalmazása, kereskedése;
- rossz minőségű termék forgalomba hozatala;[14]
- egészségügyi termék hamisítása;[15]
- fogyasztók megtévesztése;[16]
- pénzmosás;[17]
- piramisjáték szervezése;[18]
- készpénz-helyettesítő fizetési eszközök elleni támadások;[19]
- tiltott szerencsejáték szervezése.[20]

(4) A 2004. évi LXXIX. törvény az Európa Tanács Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről, amely Magyarország nemzetközi kötelezettségeit is meghatározza a kiberbűnözés elleni fellépésben.

(5) A rendőrségről szóló 1994. évi XXXIV. törvény (a továbbiakban: Rtv.) és a büntetőeljárásról szóló 2017. évi XC. törvény (a továbbiakban: Be.) a titkos információgyűjtés, illetve a leplezett eszközök vonatkozásában.

8 Btk. 197., 198., 204. §.
9 Btk. 385–388. §.
10 Btk. 384. §.
11 Btk. 375., 392–394. §.
12 Btk. 219., 375.§.
13 Btk. 176.§, 182–185.§.
14 Btk. 415. §.
15 Btk. 186. §.
16 Btk. 417. §.
17 Btk. 399. §.
18 Btk. 412. §.
19 Btk. 392–394.§.
20 Btk. 360. §.

FOGALMAK

Kibertér

Magyarország Nemzeti Kiberbiztonsági Stratégiája alapján a kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti. Magyarország kibertere a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatók, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett.[21]

Haig[22] meghatározása szerint a kibertér az ember által mesterségesen létrehozott, dinamikusan változó tartomány, amelyben az információ gyűjtését, tárolását, feldolgozását, továbbítását és felhasználását végző, egymással hálózatba kapcsolt és az elektromágneses spektrumot is felhasználó infokommunikációs eszközök és rendszerek működnek, lehetővé téve ezzel az emberek és a különféle eszközök közötti folyamatos és globális kapcsolatot.

Kiberbűncselekmény

A kiberbűncselekmény fogalma alatt az informatikai eszközök és/vagy rendszerek segítségével, vagy az informatikai eszközök és hálózatok ellen elkövetett bűncselekmények értendők, amelyek célja lehet a rendszerben tárolt adatok megszerzése, a jogosultak számára hozzáférhetetlenné tétele, továbbá az elektronikus rendszerbe vetett bizalommal történő visszaélés.[23]

Magyarországon a kiberbűncselekmények *(cybercrime)* körébe olyan cselekmények tartoznak, amelyeket számítógép, információs rendszer vagy hálózati technológia használatával követnek el.[24] A szakirodalom ennek két alapvető válfaját különíti el:

- *cyber-dependent crime:* bűncselekmények, amelyeket kizárólag számítógép segítségével lehet elkövetni (például vírusok, *hacking*);

[21] Szeleczki 2022.
[22] Haig 2018.
[23] Simon–Gyaraki 2020a.
[24] Grund 2021.

- *cyber-enabled crime:* hagyományos bűncselekmények, amelyek online környezetben, informatikai eszközökkel valósulnak meg (például csalás, zsarolás, szerzői jogsértés).

Humán információszerzés (HUMINT – Human Intelligence)

Hagyományosan a titkosszolgálatok és arra feljogosított rendvédelmi szervek emberi erőforrásokra épülő információgyűjtési módszere, amely a kibertérben új elnevezéssel, speciális megoldásokkal működik, úgynevezett CYBER-HUMINT-ként. A CYBER-HUMINT lehetővé teszi a való világban egymástól távoli, online alapú információszerzést, amely csökkentheti a kockázatokat, ugyanakkor mélyebb betekintést nyújthat a célszemély vagy -csoport tevékenységébe, jellemzőikbe. Az információgyűjtés során lehetővé válik, hogy közvetlen fizikai kapcsolat nélkül, a kapcsolattartás online térbe terelésével a tevékenységet végzők humán forrásokat foglalkoztathassanak, akár távoli földrajzi térségekben is.

A végrehajtó szervezetek tagjai szigorúan csak jogszabályi felhatalmazás alapján folytathatnak ilyen tevékenységet, Magyarországon a rendőrség vonatkozásában az Rtv. és a Be., a nemzetbiztonsági szolgálatok vonatkozásában a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény (a továbbiakban: Nbtv.), a Nemzeti Adó- és Vámhivatal vonatkozásában a róla szóló 2010. évi CXXII. törvény (a továbbiakban: NAV tv.), és szintén a Be. képezi az eljárás törvényi alapját.

A tevékenység során a HUMINT és technikai információgyűjtési módszerek integrált alkalmazása jellemző.

A kibertérben folytatott humán hírszerzés jellemzői, előnyök és hátrányok

A humán hírszerzés alkalmazása során lehetővé válik a napjainkban előszeretettel alkalmazott technikai eszközökkel nem, vagy csak részben megismerhető információk mélyebb, konspirált megismerése, az összefüggések feltárása, az érintett személyi kör pontos(abb) azonosítása. Több bűncselekménytípus esetén (például terrorizmus, kábítószeres bűncselekmények, szervezett bűnözéshez kapcsolódó bűncselekmények) jellemzővé vált, hogy az információgyűjtéssel érintett személyek köre a technikai és infokommunikációs eszközök alkalmazását illegális tevékenységeik során szándékosan minimalizálják, elkerülik, így ellehetetlenítve a technikai módszerek alkalmazásának eredményességét. A célszemélyek nem használják hagyományos infokommunikációs eszközeiket jogellenes tevékenységükkel kapcsolatos közlésekre, illetve kerülik az érzékeny információk

hagyományos hírközlő hálózaton történő továbbítását. Emellett szívesen használják az általánosan elérhető titkosítási protokollokat is, tovább nehezítve az információgyűjtéssel érintett célszemélyek kommunikációjának felderítésére és ellenőrzésére szakosodott szervezetek munkáját.[25]

Kiemelt szerepet kap a közvetlen emberi kommunikáció és a végrehajtó személyek képességei, képzettsége akár az észlelés, akár a közvetlen döntéshozatal során.

Az alkalmazási lehetőségek a humán források rendelkezésre állásától és megbízhatóságától függenek. A kapcsolatok kiépítése időigényes, hosszas előkészítést és felkészülést igényelhet. Adott esetben folyamatos, előrelátó, tervezett felderítő munkát igényelnek, amely a bűnüldöző szervek eredménykényszere vagy akár az egyes bűncselekményekhez kapcsolódó társadalmi (média-) nyomás esetén nem tud maradéktalanul érvényesülni.

A kibertérben folytatott információszerzés területén már most is a fiatalabb generációk dominanciája tapasztalható, hiszen a kibertér működése, jellemzői, a technológiai környezetből érkező információk értelmezése, a social media működése, a különböző információ- és kommunikációtechnológiai megoldások alkalmazása számukra magától értetődő. Ebben a vonatkozásban (is) komolyan felmerül a végrehajtó állomány utánpótlásának, illetve az együttműködők kiválasztása feltételei megváltozásának a kérdése.

A működési költségei alacsonyabbak a technikai megoldásokhoz viszonyítva.

A végrehajtó állomány, illetve az alkalmazott együttműködők kevésbé vannak közvetlen veszélynek kitéve.

A valós térben játszódó humáninformáció-szerzés és a virtuális térben megvalósuló humáninformáció-szerzés különböző képességeket, felkészültséget, előkészítő munkát igényel. A valós és a virtuális térben folytatott felderítés kiegészítheti egymást, mégis különböző nehézségeket és feladatokat jelent a bűnüldöző szerveknek. Ha például arra gondolunk, hogy az online térben a felhasználók gyakran valótlan információkat osztanak meg magukról, a felhasználónevek, profilok, avatárok mögötti természetes személyek azonosítása a felderítés egyik alapkérése lesz, ugyanakkor ugyanez a magatartás a végrehajtó állomány vagy az együttműködők leplezését, legendájának kialakítását egyszerűbbé teszi.

A valós és a virtuális térben folytatott humáninformáció-szerzést árnyalja, hogy napjainkban már számos információ alapvetően nyílt, technikai jellegű forrásban áll rendelkezésre – amelyek OSINT (*open-source intelligence,* azaz nyílt forrású információgyűjtés) útján is beszerezhetők –, illetve az emberi kapcsolatokat előtérbe helyező közösségi oldalakon is hozzáférhetők – akár az

[25] Dobák–Tóth 2021.

úgynevezett SOCMINT (*social media intelligence,* vagyis közösségi médiából történő információgyűjtés) során.[26]

Elkövetők

Az online tér megnyitotta a teljes anonimitás lehetőségét, a büntetlenség érzését kölcsönző anonimitását. Kezdetben a kiberbűnözők olyanokból lettek, akik szaktudással rendelkeztek a számítógépes nyelvezetek, programozástudomány vagy hálózati architektúra terén, és képesek voltak technikailag összetett, bonyolult bűncselekmények elkövetésére. A számítógépes ismeretek és alkalmazások általános(abb)á válásával megjelentek az egyéb, nem professzionális kiberbűnözők. Ők kisebb technikai tudással és szakértelemmel rendelkeznek, ugyanakkor ismereteik elégségesek ahhoz, hogy kapcsolatot tartsanak egymással, megszervezzék bűnös tevékenységüket, esetleg megvásárolják hozzá mindazt a speciális tudást és eszközparkot, ami az eredményes működésükhöz szükséges. A számítógépes rendszerek egyre inkább megkerülhetetlen részét képezik a személyes és üzleti életünknek, egyre többen képesek megérteni a kibertér alapvető jelentőségét és az általa kínált (potenciálisan jogsértő) lehetőségeket. Ugyanakkor kialakult egyfajta szolgáltatóipar – mondjuk a *dark weben* –, amely a bűncselekmények elkövetéséhez szükséges szoftvereket, tudást, egyéb eszközöket, hamis személyazonosságot biztosítja a bűnelkövetők számára.

A HUMÁN HÍRSZERZÉS LEHETŐSÉGEI A KIBERTÉRBEN

A Be. a leplezett eszközök körében lehetővé teszi a humán információszerzést a büntetőeljárás során, egyrészt a titkosan együttműködő személy igénybevételével,[27] másrészt az ügyészi engedélyhez kötött leplezett eszközök között a fedett nyomozó alkalmazásával.[28]

A törvényben felsorolt célok közül a kibertérben a fedett nyomozó bűnszervezetbe történő beépülés, terroristacsoportba történő beépülés, álvásárlás, dezinformáció továbbítása vagy a bűncselekménnyel összefüggő információk és bizonyítékok megszerzése érdekében alkalmazható.[29]

A fedett nyomozó a kibertérben folytatott tevékenységéhez kapcsolódó bűncselekmény, szabálysértés vagy közigazgatási bírsággal sújtandó szabályszegés

[26] Dobák–Tóth 2021.
[27] Be. 215. § (1).
[28] Be. 222–225. §.
[29] Be. 222. § (2).

miatt nem büntethető (amennyiben az elkövetett jogsértés a törvényben meghatározott célokat segíti elő, azaz az alkalmazás eredményességét, a fedett nyomozó biztonságát, vagy más bűncselekmény megelőzését szolgálja).[30] Az ehhez kapcsolódó törvényi korlátozások a kibertérben nem életszerűek (a fedett nyomozó nem követhet el más életének szándékos kioltásával járó, illetve maradandó fogyatékosságot vagy súlyos egészségromlást szándékosan okozó bűncselekményt).[31] Ugyanakkor tevékenysége a kibertérben sem bírhat rá mást bűncselekmény vagy az eredeti szándékánál súlyosabban minősülő bűncselekmény elkövetésére.[32]

A titkosan együttműködő személyek közül az informátorral és a titkos munkatárssal érdemes a kibertérben folytatott humán információszerzés kapcsán foglalkozni. Mivel a két együttműködői kategória között meglévő különbségek (együttműködés időbelisége, mélysége, az együttműködő személy megbízhatósága) jelen publikáció szempontjából nem releváns, a továbbiakban az érthetőség kedvéért az informátor kifejezést fogom használni.

Vitathatatlan, hogy a kibertérben folytatott humán hírszerzés egyik sarkalatos pontja a hatóságok oldalán ilyen tevékenységet folytató személy szakértelme, informatikai jártassága. Amennyiben a fedett nyomozónk rendelkezik ezekkel az ismeretekkel, képességekkel, a mögötte álló jogszabályi felhatalmazással és szervezeti támogatással gyakorlatilag probléma és korlátozás nélkül tudja a tevékenységét folytatni a kibertérben. A bűnüldöző szervek folyamatos képzéssel, továbbképzéssel igyekeznek közelíteni ehhez az ideális állapothoz, azonban még sokáig szükséges lesz egyéb, megfelelő ismeretekkel rendelkező (a már említett informatikai-technikai ismeretek, a célszemélyhez, csoporthoz kapcsolódó személyi ismeretek, a bűncselekmény elkövetéséhez kapcsolódó gazdasági, műszaki és egyéb ismeretek) együttműködők igénybevételére is.

Az egyéb együttműködők tekintetében kardinális kérdés a bűncselekmény elkövetésének lehetősége, amelyet a jelenlegi törvényi szabályozás nem tesz lehetővé. A kibertérben – mondjuk a *dark weben* vagy a közösségi hálókon, illetve egyéb informatikai rendszerekhez kapcsolódóan végzett felderítő munka során – az informátor szinte szükségszerűen bűncselekményt követ el (gyermekpornográfia, szervezett bűnözéshez kapcsolódó tevékenységek, jelszavak, profilok feltörése, egyéb – a felderítés szempontjából releváns – adatok megszerzése), de mindenképpen olyan szürke zónában tevékenykedik, ami felvetheti az együttműködőnk büntetőjogi felelősségét.

30 Be. 224. §.
31 Be. 224. § (3).
32 Be. 224. § (4.)

Megoldást jelenthet a Be. módosítása és az álvásárlás[33] mintájára lehetővé tenni az együttműködő személynek (vagy a hatóság nem fedett nyomozó minőségben eljáró tagjának), hogy a kibertérben folytatott felderítő tevékenysége során, előzetes ügyészi engedéllyel bizonyos bűncselekményeket elkövethessen (azzal, hogy ebben az esetben rá is a fedett nyomozóra vonatkozó szabályok megfelelően alkalmazandók).[34]

Néhány kiegészítő gondolat

Amennyiben a kibertérben (is) tevékenykedő (szervezett bűnözői) csoport a való világban is működik, megvan a vezetők, csoporttagok közötti személyes kapcsolat is, természetesen a hagyományos humán hírszerzés megoldásai is alkalmazandók.

A kibertérben folytatott humáninformáció-szerzés esetében a személyes kapcsolat hiánya előny és hátrány is lehet. Előny például a fedett nyomozó, vagy ha szükséges, az együttműködő személy legendájának kialakításánál, ugyanakkor hátrányt jelenthet az elkövetővel való kommunikációban, a célszemély azonosításában.

A már említett szolgáltatásnyújtáshoz kapcsolódva elképzelhető, hogy egy ilyen személy több más bűnös tevékenységet folytató személyhez vagy csoporthoz is kapcsolódik. Ezeknek a csomópontoknak a felderítése eredményesebbé teheti a felderítést, kiterjesztheti annak irányát.

A kibertérben a szervezett bűnözésre jellemző területi viták nehezebben jöhetnek létre.[35]

A kibertérben jelen vannak az egyéni elkövetők is, de egyre inkább jellemző a csoportban történő elkövetés, hiszen egy-egy bűncselekmény elkövetése jellemzően többirányú felkészültséget, ismereteket igényel. Köszönhetően a hatóságok munkájának, az informatikai rendszerek üzemeltetői magasabb szintű védekezésének, az állampolgárok tudatossága növekedésének (?) az egyéni, ötletszerű elkövetőknek egyre kisebb az esélyük sikeresen működni.

Egy kibertérben működő szervezett bűnözői csoport működhet nagyon strukturált, hagyományos maffiaszerű csoportként, amely bűnöző informatikai szakembereket vonz. Elképzelhető, hogy egy meghatározott cél érdekében létrejön egy szigorúan konspirált bűnözői csoport, de az eddig megismert esetekben ezek egy-egy konkrét bűncselekmény, egy konkrét sértett ellen vagy cél érdekében

[33] Be. 221. §.
[34] Be. 226. §.
[35] Simon-Gyaraki 2020b.

szerveződnek, tehát nem tartós jellegű együttműködés, hanem sokkal inkább a projektszemlélet uralkodik.[36]

ZÁRÓ KÖVETKEZTETÉSEK

A kibertérben folytatott humán információszerzés egy új, gyorsan fejlődő szakterület, amely a klasszikus HUMINT-módszereket és az új digitális eszközöket, az online világ lehetőségeit ötvözi.

A magyar jogi szabályozás biztosítja az alapvető kereteket a felderítéshez, az adatok védelméhez és a kiberbiztonsági követelmények teljesüléséhez, azonban a technológiai fejlődés miatt folyamatosan szükséges a szabályozások és gyakorlatok frissítése.

A jövőben a humán és technikai információszerző módszerek integrált alkalmazása kulcsfontosságú lesz a hatékony, jogszerű és etikus kibertéri (humán) információszerzés érdekében.

BIBLIOGRÁFIA

Dobák Imre – Tóth Tamás (2021): Régi módszerek a kibertérben? (CYBER-HUMINT, OSINT, SOCMINT, Social Engineering). *Belügyi Szemle,* 69(2), 195–212. Online: https://doi.org/10.38146/BSZ.2021.2.2

Grund Borbála (2021): A kibertér bűncselekményeiről és a kiberbűnözés hazai gyakorlatáról. *MTA Law Working Papers,* 8(21), 1–37.

Haig Zsolt (2018): *Információs műveletek a kibertérben.* Budapest: Dialóg Campus.

Simon Béla (2017): A bűnüldözés előtt álló digitális kihívások. *Magyar Rendészet,* 17(5), 83–103. Online: https://real.mtak.hu/216958/1/marczikaz.pdf

Simon Béla – Gyaraki Réka (2020a): Kiberbűncselekmények felderítése és nyomozása. In Kiss Tibor (szerk.): *Kibervédelem a bűnügyi tudományokban.* Budapest: Dialóg Campus, 121–150. Online: https://doi.org/10.36250/00782_08

Simon Béla – Gyaraki Réka (2020b): Kiberbűnözés. In Kiss Tibor (szerk.): *Kibervédelem a bűnügyi tudományokban.* Budapest: Dialóg Campus, 95–119. Online: https://doi.org/10.36250/00782_07

Szeleczki Szilveszter (2022): A kiberhírszerzés értelmezése és helye a nemzetbiztonságban. *Nemzetbiztonsági Szemle,* 10(4), 17–29. Online: https://doi.org/10.32561/nsz.2022.4.2

[36] Simon 2017.

Jogszabályjegyzék

1994. évi XXXIV. törvény a rendőrségről.
1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról.
2004. évi LXXIX. törvény az Európa Tanács Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről.
2010. évi CXXII. törvény a Nemzeti Adó- és Vámhivatalról.
2012. évi C. törvény a Büntető Törvénykönyvről.
2017. évi XC. törvény a büntetőeljárásról.
2024. évi LXIX. törvény Magyarország kiberbiztonságáról.
1089/2025. (III. 31.) Korm. határozat Magyarország Kiberbiztonsági Stratégiájáról.